

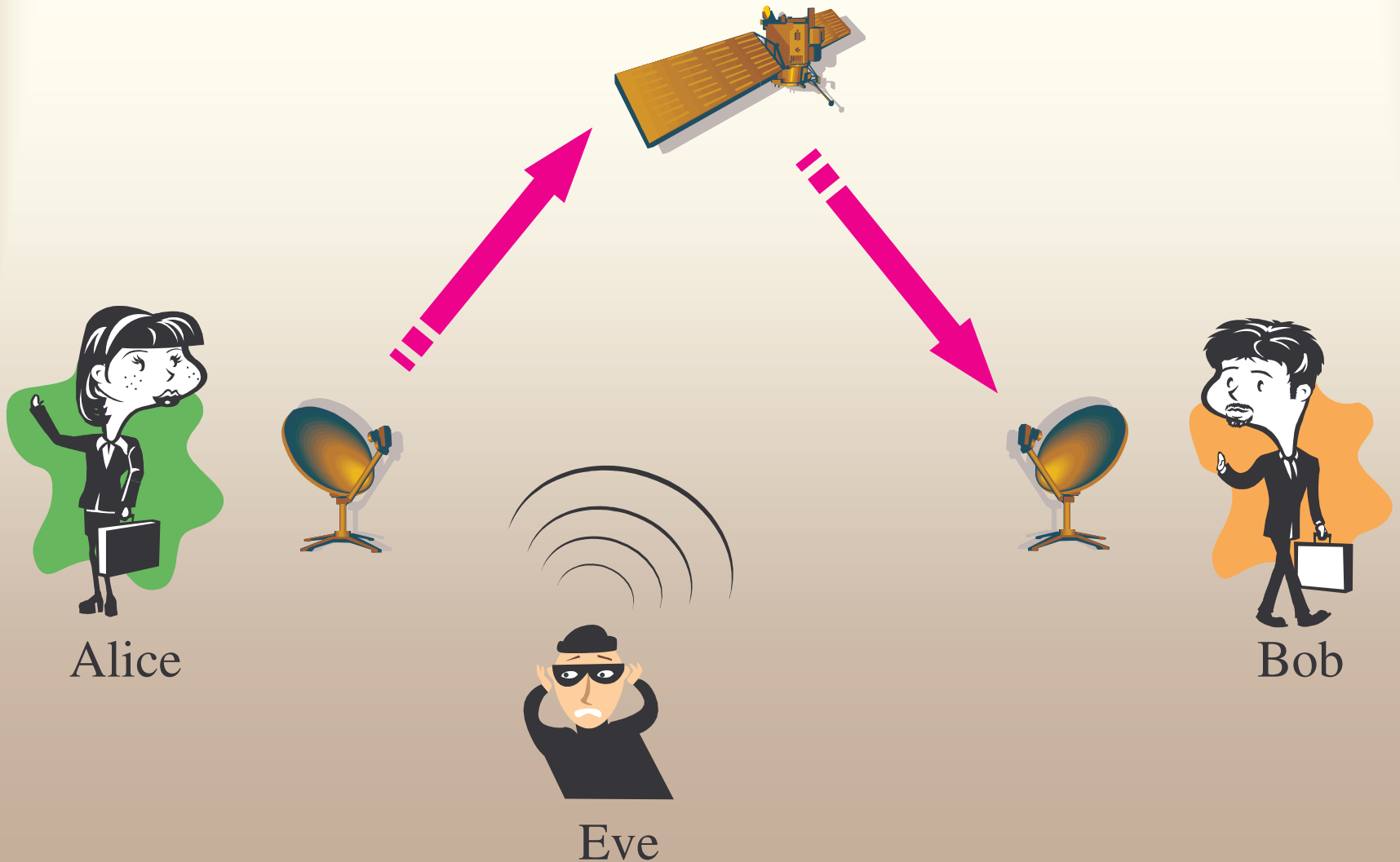
Cryptography

Plan

- Presentation
- Symmetric Encryption
- Asymmetric Encryption
- Zero knowledge proofs

Presentation

Secure (Encrypted) channel

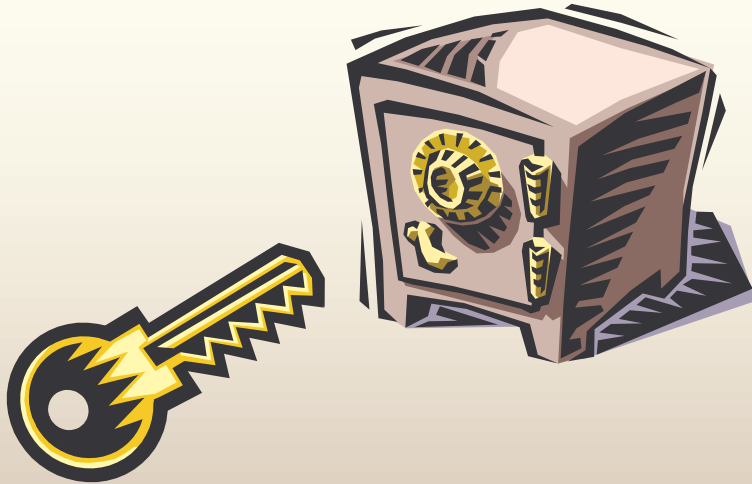


Presentation

Secure data



Alice



Eve

Presentation Signature



Alice



Bob

Presentation

Other

- Identification
- Integrity
- Involved functions
 - Credit card payment
 - Payment on the Internet
 - Electronical voting system
 - ...

Symmetric Encryption



Alice



Bob

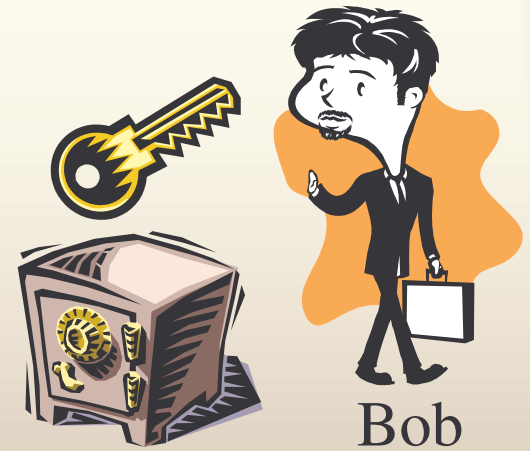


Eve

Symmetric Encryption



Symmetric Encryption



Symmetric Encryption

Cesar Cryptosystem

- Three-letter shift
- Example
 - Plaintext: Attack now!
 - Cyphertext: DWWDFN QRZ!

Symmetric Encryption

Perfect Cryptosystem

- Value of letters: A=1, B=2 ... Z=26
- Add key and plaintext.
 - Ex: $T+L=20+12=32=26+6=F$
- Example
 - Plaintext: This is a secret
 - Key: Lock

THISISASECRET	
+LOCKLOCKLOCKL	
FWLDUHDDQRUPF	

Symmetric Encryption

Perfect Cryptosystem

- Perfect Cryptosystem
 - Key Length = Plaintext Length
 - Cannot decrypt with infinite computation power
- Example
 - Plaintext: **DOGS** and Key: SURE
 - Cyphertext: DOGS+SURE=WJYX
 - Eve's Key: TUBE
 - Eve's decrypt: **COWS** (COWS+TUBE=WJYX)

Symmetric Encryption

Current Cryptosystem

- AES: Advanced Encryption Standard (2000)
 - Mix several times key and plaintext
 - Complex method
 - Knowledge of Plaintext and Cyphertext



Knowledge of the key

Symmetric Encryption Problem

- Alice and Bob : same key
- How does Alice send the key?
- Alice and Bob : know each other?
- What append when Eve gets the key?
- ...

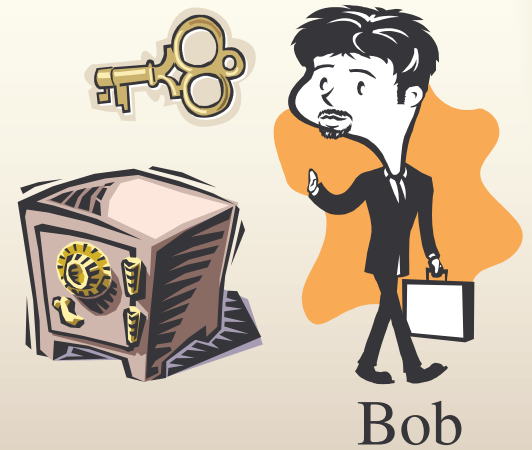
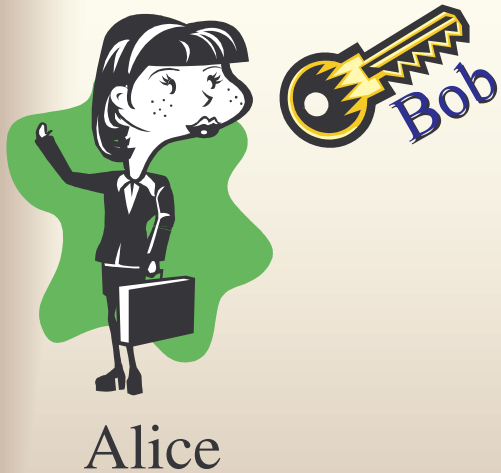
Asymmetric Encryption



Asymmetric Encryption



Asymmetric Encryption



Asymmetric Encryption

- Two keys
 - Public key
 - Private key
- Use mathematical functions
 - One-way functions
 - Trapdoor
- Need high computation power to deduce the plaintext from the cyphertext (try all private keys)

Asymmetric Encryption

RSA

- Rivest, Shamir, Adleman (1978)
 - Most of algorithms based on RSA
 - Use difficulty of factorization of large numbers
 - Private key: 2 large prime numbers p, q
 - Public key: $n = p * q$
 - Plaintext m , cyphertext $c = f(m, n)$
 - Decrypt: $m = g(c, p, q)$

Asymmetric Encryption

Signature

- Asymmetric encryption scheme



Signature scheme

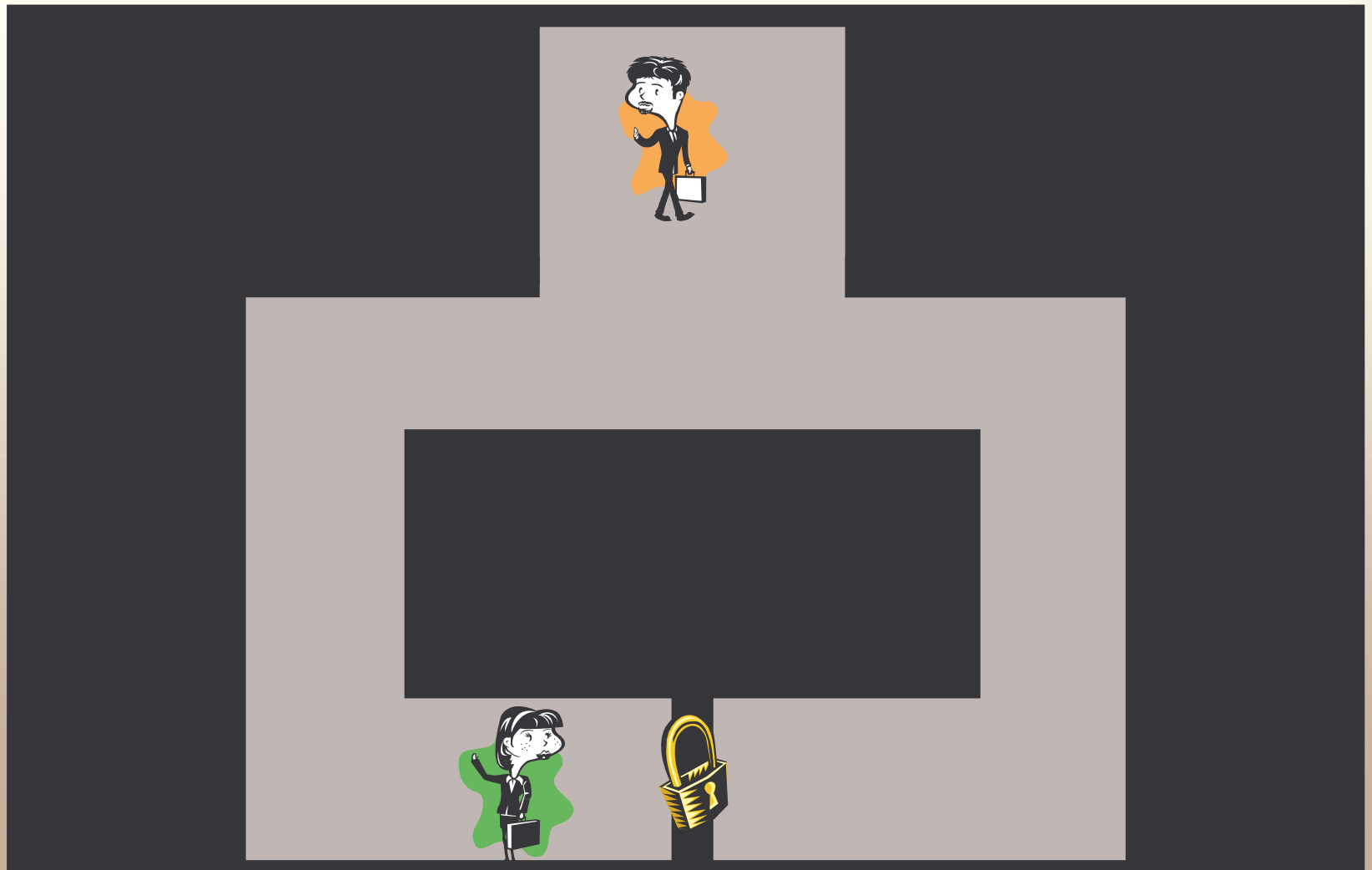
- Encryption: $c=f(PK,m)$ $m=g(SK,c)$
- Signature: $s=g(SK,m)$
- Send m and s
- Verify: $f(PK,s)=m$

Zero knowledge proof

- Alice wants to prove to Bob, she knows a secret
- Eve spy the communications
- Alice is not sure Bob is honest

Zero knowledge proof

Cave allegory



Zero knowledge proof

Cave allegory

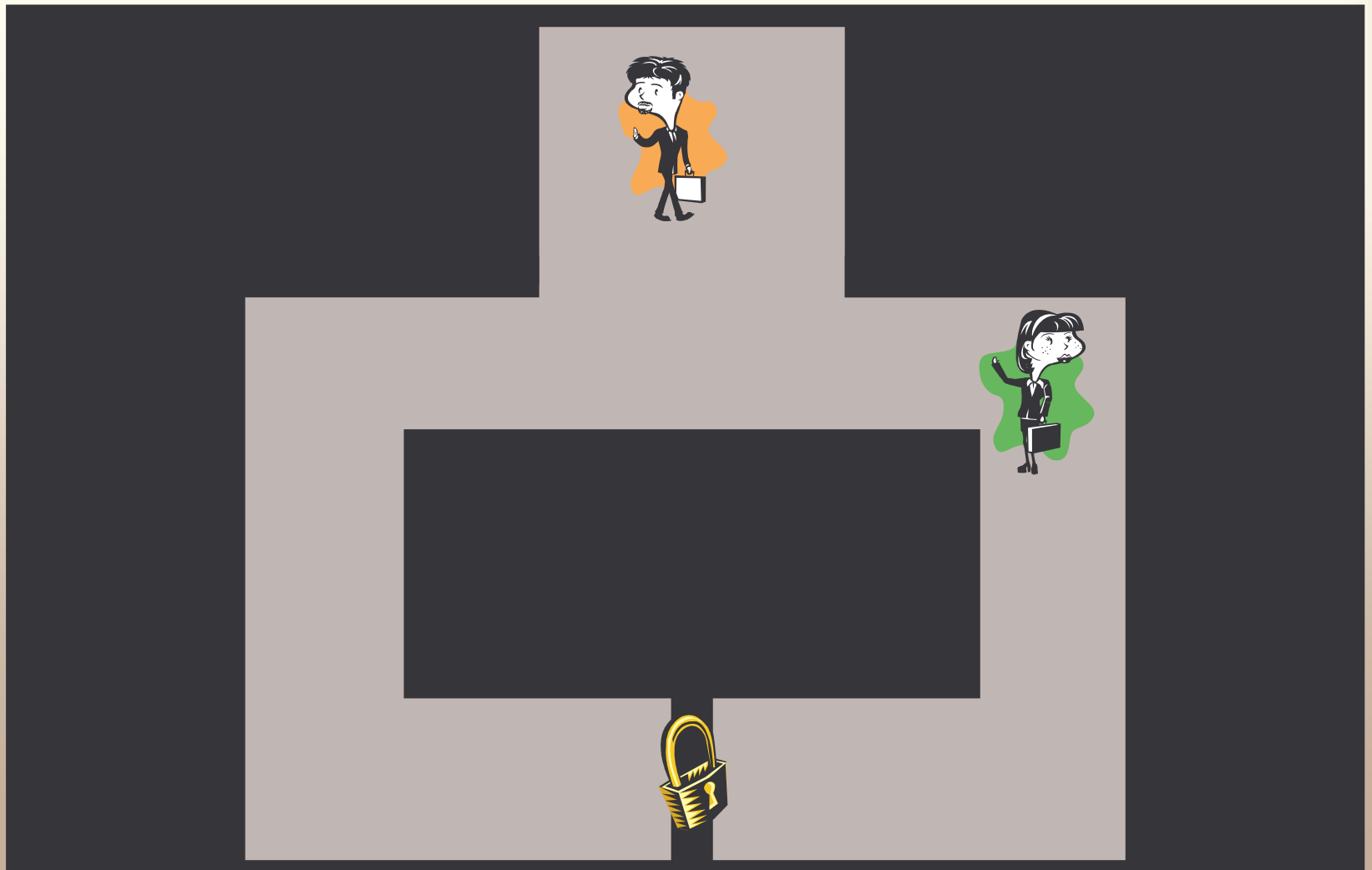


Right



Zero knowledge proof

Cave allegory



Conclusion

- Simple ideas
- Complex mathematical functions
- Large spread